Curbing Crypto Wallet Fraud

Blockchain is becoming the new frontier for secure transactions. However, that doesn't necessarily mean blockchain solutions are managed securely.

Because blockchain technology is continuously evolving, and due to its decentralized nature, there is no uniform guidance for building secure blockchain solutions. The lack of information and experience is leading Crypto providers to develop technology that is based on what they think is ideal or suitable.

While some crypto wallet providers incorporate effective security controls and processes, others may not, elevating risk of the technology being compromised as well as anything built on top of it.

The recent wave of crypto account takeover attacks has shed a light on one of the most vulnerable and penetrable points in the crypto payment process – the registration and login.

Paygilant secures the entire crypto-user journey, from app download, through registration, enrollment, login, to payment. Paygilant ensures that users credentials cannot be falsified or compromised, providing maximum confidence to users and wallet providers alike.

Value for Wallet Providers

- **Provides maximum security throughout the Crypto Wallet user journey – from app download, registration, login to transaction.**

- **Enables an interruption-free crypto wallet user experience.**

- **Mitigates Crypto Wallet Account Takeover**

- **Identifies sparks of crypto fraud before it happens**

Username/password - the weakest link in the Crypto Wallet login process

Using phishing attacks, fraudsters have preyed on crypto wallet users specifically during login, falsifying username/password and gaining access to their private wallets.

A common attack MO that has victimized crypto wallet users is combination of SIM swap and account takeover fraud, that exploits two-factor authentication protection by hijacking the SIM card on their mobile device. Criminals usually obtain a username/password by exploiting mobile operators' ability to port any mobile number onto a blank SIM card.

How Does Paygilant Secure Crypto Wallets Throughout The User's Journey

Paygilant provides comprehensive security throughout the crypto wallet users journey, anticipating and preventing fraud at multiple checkpoints. Paygilant's six intelligence sets work as layers, using a combination of behavioral biometrics, device fingerprinting and transaction data to stop crypto fraud.

Users' Journey

App Download	Onboarding/Registration	Login	Transaction
1	2	3	4

Paygilant's six intelligence sets

How Paygilant helps stop Crypto Fraud

During the app download stage, Paygilant analyses and cross-refences the mobile device (contacts, pics, Wifi networks, etc.) and users' data to identify anomalies that might be pre-cursors of crypto fraud.

In the registration stage, Paygilant's four intelligence sets kick-in, evaluating and correlating device activity, along with app interactions and bio markers to determine if device has been tampered (SIM SWAP) and/or account takeover may be attempted.

In the login stage, five intelligence sets are triggered, and heightened analysis of attack MO's is performed.

All six inelegance sets are triggered, and a risk score indicates if the crypto transaction is legitimate or fraudulent. Only in the likelihood that the transaction is fraudulent, step-up authentication will be triggered.